BIRCH, STEWART, KOLASCH & BIRCH, LLP

TERRELL C. BIRCH
RAYMOND C STEWART
JOSEPH A KOLASCH
JAMES M SLATTERY
BERNARD L SWEENEY*
MICHAEL K MUTTER
CHARLES GORENSTEIN
GERALD M MURPHY, JR.
LEONARD R. SVENSSON
TERRY L CLARK
ANDREW D. MEIKLE
MARC S WEINER
JOE McKINNEY MUNCY
ROBERT J KENNEY
DONALD J DALEY
JOHN W BAILEY
JOHN A CASTELLANO, III
GARY D YACURA

OF COUNSEL
HERBERT M. BIRCH (1905-1996)
ELLIOT A GOLDBERG*
WILLIAM L GATES*
EDWARD H VALANCE
RUPERT J BRADY (RET)*
F. PRINCE BUTLER
FRED L. WHISENHUNT
*ADMITTED TO A BAR OTHER THAN VA

INTELLECTUAL PROPERTY LAW
8110 GATEHOUSE ROAD
SUITE 500 EAST
FALLS CHURCH, VA 22042-1210
USA

(703) 205-8000

FAX (703) 205-8050
(703) 698-8590 (G IV)

e-mail: mailroom@bskb.com
web: http://www.bskb.com

CALIFORNIA OFFICE
COSTA MESA, CALIFORNIA

THOMAS S. AUCHTERLONIE
JAMES T ELLER, JR
SCOTT L LOWE
MARK J NUELL, PH.D.
D RICHARD ANDERSON
PAUL C LEWIS
MARK W MILSTEAD*
JOHN CAMPA*
RICHARD J GALLAGHER

REG PATENT AGENTS
FREDERICK R. HANDREN
MARYANNE ARMSTRONG, PH.D
MAKI HATSUMI
MIKE S. RYU
CRAIG A. McROBBIE
GARTH M DAHLEN, PH D
LAURA C LUTZ
ROBERT E. GOOZNER, PH D
HYUNG N SOHN
MATTHEW J. LATTIG
ALAN PEDERSEN-GILES
JUSTIN D KARJALA
C. KEITH MONTGOMERY
TIMOTHY R WYCKOFF
HERMES M. SOYEZ, PH D
KRISTI L RUPERT, PH.D

June 12, 2000
2950-0160P

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

As authorized by the inventor, transmitted herewith for filing is a continuation reissue application of a reissue application 09/094,575 filed June 12, 1998 (Attorney Docket No.: 2950-0142P) for and on behalf of the inventor(s) according to the provisions of 37 C.F.R. § 1.171.

Inventor(s): **Tae Joon PARK**

For: COPY PREVENTION METHOD AND APPARATUS OF A DIGITAL MAGNETIC RECORDING/REPRODUCING SYSTEM

Enclosed are:

X A reissue application of U.S. Patent No. **5,689,559** consisting of **THIRTY-ONE (31)** pages.

__ sheet(s) of _____ drawings

_ Certified copy of _____

_ Executed Declaration (_ Original _ Photocopy)

_ A verified statement (__ Original __ Photocopy) to establish small entity status under 37 C.F.R. § 1.19 and 37 C.F.R. § 1.27.

X Information Disclosure Statement and PTO-1449

_ Information Sheet

X Assent of Assignee to Reissue; Establishment of Ownership under 37 C.F.R. §3.73(b)

X Reissue Declaration

The filing fee has been calculated as shown below:

			LARGE ENTITY	SMALL ENTITY
	BASIC FEE		$690.00	$395.00
	NUMBER FILED	NUMBER EXTRA	RATE FEE	RATE FEE
TOTAL CLAIMS	31-20 =	11	11 x 18 = $198.00	x 11 = $
INDEPENDENT CLAIMS	6 - 3 =	3	3 x 78 = $234.00	x 41 = $
MULTIPLE DEPENDENT __ CLAIMS PRESENTED			+ $.00	+ $135.00
		TOTAL	$1122.00	

_ The application transmitted herewith is filed in accordance with 37 C.F.R. § 1.41(c). The undersigned has been authorized by the inventor(s) to file the present application. The original duly executed Declaration together with a surcharge will be forwarded in due course.

X A check in the amount of **$1122.00** to cover the filing fee is enclosed.

_ Please charge Deposit Account No. 02-2448 in the amount of $_____. A triplicate copy of this transmittal form is enclosed.

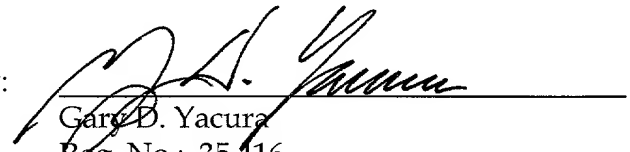
X Send correspondence to:

BIRCH, STEWART, KOLASCH & BIRCH, LLP
P.O. Box 747
Falls Church, Virginia 22040-0747

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§§1.16, 1.17 or 1.19; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By: 

Gary D. Yacura
Reg. No.: 35,416

GDY:jcp

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

PATENT
2950-0160P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS: Tae Joon PARK

APPLICATION. NO.: NEW CONTINUATION APPLICATION OF USSN 09/094,575, WHICH IS A REISSUE APPLICATION OF U.S. Pat. No. 5,689,559

FILING DATE:

(Issued: November 18, 1997)

FOR: COPY PREVENTION METHOD AND APPARATUS OF A DIGITAL MAGNETIC RECORDING/REPRODUCING SYSTEM

ASSENT OF ASSIGNEE TO REISSUE PATENT NO. 5,689,559

The undersigned, assignee of the entire interest of U.S. Patent No. 5,689,559 by virtue of an Assignment duly recorded in the Assignment Records of the U.S. Patent and Trademark Office on **April 26, 1996** at Reel **7912**, Frame(s) **0579**, hereby assents to the accompanying continuation reissue application.

LG ELECTRONICS INC.

Date: June 8, 2000 By: Paek Bok Kyun
(Signature)

Manager
(Title)

Related Application

This reissue application is a continuation of reissue application no. 09/094,575 filed on June 12, 1998.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a copy prevention method and apparatus of a digital [magnetic] recording/reproducing system, and more particularly to a copy prevention method and apparatus of a digital [magnetic] recording/reproducing system, wherein a marker [involving copy prevention function information and executing the function is coded and inserted to perform the copy prevention function and realize the copy prevention function of various patterns desired by a program supplier] includes control data for descrambling digital data.

2. Description of the Prior Art

One example of a conventional copy prevention method is described in U.S. Pat. No. 4,819,098, in which a signal inducing an interference to an automatic gain controller (AGC) circuit within a VCR is inserted to a video waveform to be recorded on a tape. When the tape is reproduced to display the signal on a television, the interference signal does not affect the AGC circuit of the television, [to allow] allowing for a normal display.

However, when the reproduced signal is recorded by another VCR, i.e., when it is duplicated, the interference signal brings about [the] interference in the AGC circuit of the recording VCR causing [to record in] an inaccurate signal level to be recorded. Accordingly, the nodal display cannot be attained when reproducing a duplicated tape.

As another example, U.S. Pat. No. 4,571,642 utilizes a control track employed during performing the reproduction for synchronizing a servo circuit within a VCR, [thereby] for embodying the copy prevention function. The basic concept of this patent is for altering a video signal to force the control track to be inaccurately recorded when the video signal is duplicated onto another tape.

Still another example is disclosed in U.S. Pat. No. 4,577,216, in which a phase noise or the like is inserted [to] in a chroma burst portion of a video signal to thereby embody the copy prevention function.

The above-mentioned methods [are for using] use a difference between the [of] sensitivity [between] of circuits [of] in a television and [of] a VCR. [Thus, the copy prepared to prevent the copy thereof as above may not exert the copy prevention function in a certain VCR, but may not execute a normal display on a certain television.]

The above copy prevention methods are of an analog system, which are available for preventing the copy of an NTSC-class video signal to an analog VCR. However, in case of a high-definition image of the analog television (ATV), the copy is performed by means of a digital VCR rather than an analog VCR, so that it is difficult to employ the copy prevention method of the analog system.

SUMMARY OF THE INVENTION

Therefore, it is an object of the present invention to provide a copy prevention method and apparatus of a digital [magnetic] recording/reproducing system [applicable to a digital VCR and incorporated with various copy prevention functions to enable the selection of a copy prevention function desired by a program supplier.

To achieve the above object of the present invention, there is provided a copy prevention method of a digital magnetic recording/reproducing system, which is performed by an audio and video signal transmitting process and an audio and video signal receiving/recording process. The audio and video signal transmitted process is carried out in the sequence of encrypting a marker formed by a control word for scrambling audio and video bit strips and copy prevention information for preventing an illegal copy by means of an encoding key, and multiplexing the marker with the audio and video bit strips scrambled by the control word. Then, the audio and video signal receiving/recording process is performed in the sequence of detecting the marker from the transmitted bit strips, decrypting and analyzing the detected marker by means of an encoded key to determine whether [copy] copying is permitted or not, updating the detected marker to be recorded on a video tape, and generating the control word from the marker to perform a descrambling and supply the audio and video signals to be displayed on a monitor.

Also, a copy prevention apparatus of a digital magnetic recording/reproducing system includes a marker detecting and inserting part for detecting a marker from input bit strips, and inserting the updated marker to the bit strips to output the result. A marker analyzing and processing part decrypts and analyzes the encrypted marker from the marker detecting and inserting part by means of an encoded key, outputs a control word for descrambling the bit strips, and updates and encrypting the decrypted marker by means of the encoded key to output the result. In addition, a buffer part buffers the control word and updated and encrypted marker from the marker analyzing and processing section, and inserts the updated and encrypted marker in the marker detecting and inserting part, and a descrambler descrambles the bit strips provided via the marker detecting and inserting part by means of the control word from the buffer part.]

These and other objects are achieved by providing a method of copy protecting digital data, comprising generating copy prevention information; generating control data; scrambling digital data based on said control data; forming a marker, said marker including said copy prevention information and said control data; and transmitting said scrambled digital data and said marker.

These and other objects are further achieved by providing a method of processing copy protected digital data, comprising receiving digital data said digital data including copy prevention information; determining from said copy prevention information whether copying is permitted; updating said copy prevention information if said determining step determines that a copy is permitted; inserting said updated copy prevention information in place of said copy prevention information only in said digital data for recording; and recording output from said inserting step.

These and other objects are still further achieved by providing an apparatus for copy protecting digital data, comprising a copy prevention generator generating copy prevention information; a control data generator generating control data; a scrambler scrambling digital data based on said control data; marker forming means for forming a marker, said marker including said copy prevention information and said control data; and a transmitting unit transmitting said scrambled digital data and said marker.

In an alternative embodiment, the scrambled digital data and the marker are recorded.

These and other objects are still further achieved by providing an apparatus for processing copy protected digital

data, comprising a receiving unit receiving digital data, said digital data including copy prevention information; an analyzing unit determining from said copy prevention information whether copying is permitted, and updating said copy prevention information if a copy is permitted; an inserting unit inserting said updated copy prevention information in place of said copy prevention information only in said digital data for recording; and a recording unit recording output from said inserting unit.

BRIEF DESCRIPTION OF THE DRAWINGS

The above objects and other advantages of the present invention will become more apparent by describing in detail preferred embodiments thereof with reference to the attached drawings in which:

FIG. 1 is a flow chart illustrating an audio and video signal transmitting process in a copy prevention method according to the present invention;

FIG. 2 is a flow chart illustrating an audio and video signal receiving and recording process in the copy prevention method according to the present invention;

FIG. 3 is a view showing a structure of transport bit strips according to the present invention;

FIG. 4 is a block diagram showing a schematic construction of a copy prevention apparatus according to the present invention;

FIG. 5 is a block diagram showing a detailed construction of FIG. 4; and

FIGS. 6A to 6F are signal waveforms of respective parts shown in FIG. 5.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A copy prevention method and apparatus of a digital [magnetic] recording/reproducing system according to the present invention [emphasizes a fact that a DVCR can record all diverse signals on a video tape, so that a variety of input signals are largely classified into two, and different] use a copy prevention [methods are performed for each signal] method based on the type of input signal.

First, signals transmitted from a terrestrial broadcasting system, a satellite broadcasting system and a pay television broadcasting system are classified as [a] broadcasting [signal] signals, and the following three copy prevention functions are applicable when recording [the] a broadcasting signal.

The three [Three] copy prevention functions are a no recording permitted [onto a video tape], a free record/copy [onto the tape], and a single generational recording [onto the tape with no copy of the recorded tape].

Here, the third copy prevention function [of the single generational recording onto the video tape with no duplication of the recorded tape] is for enabling the signal from a television receiver to be recorded [record on the tape] once but [inhibiting] the re-recording of the signal by means of, for example, [another] a DVCR is prohibited while the firstly-recorded [tape] signal can be reproduced to watch through a monitor.

A second classification is for, for example, a rental tape to be identified by a pretaped signal. Here, the copy prevention function of the pretaped signal is similar to the above no recording [onto the tape] and the free record/copy copy protection function [onto the tape], [which] and has the following three copy protection functions.

The three functions are no copy onto another tape, free copy to another tape and a single generational copy to another tape.

The single generational copy function [to the other tape is of the copy prevention function for allowing a] allows duplication from the original [rental tape], but inhibits [inhibiting] another copy from the [duplication] duplicate[, which is utilized in a digital audio tape (DAT)].

The present invention is advantageous in that a program supplier selects the above functions when providing a program. For this purpose, the program supplier inserts desired copy prevention function information, i.e., a marker, into a predetermined field within the program.

The marker inserted [to transport data] by the program supplier prior to being transmitted is encoded, and, in order to impede an illegal copy, an encoding key for interpreting the marker is transferred via a separate transmission line such as telephone line by a prescribed period interval, e.g., once a month, to be stored within a copy prevention apparatus.

In a system having an ATV decoder incorporated in a body with, for example, the DVCR [in a body], a copy prevention apparatus for embodying the copy prevention functions executes a digital copy prevention function during an interface process between the ATV decoder and the DVCR. [, and] The copy prevention apparatus decodes and determines the marker of a received program by means of a received [encoded] encoding key to perform another function in accordance with respective copy prevention functions.

The copy prevention method of the digital [magnetic] recording/reproducing system according to the present invention is performed through an audio and video signal transmitting process as shown in FIG. 1, and an audio and video signal receiving and recording process as shown in FIG. 2.

The audio and video signal transmitting process is for encrypting the marker formed by a control word for scrambling audio and video bit strips and copy prevention (hereinafter simply referred to as "CP") information for preventing an illegal duplication by means of an encoded key to multiplex and transmit the audio and video bit strips scrambled by the control word. Here, the marker is already formed by a program producer to be multiplexed and transmitted together with the audio and video bit strips.

In more detail, as shown in FIG. 1, the audio and video signal transmitting process is carried out in the sequence of an audio/video bitstrip encoding step 1 for encoding the audio and video bit strips, a control word generating step 2 for generating the control word for scrambling, and a scrambling step 6 for scrambling the encoded audio and video bit strips by means of the generated control word. Successively, a CP information generating step 3 generates the CP information for preventing the illegal copy, and marker producing and encrypting steps 4 and 5 respectively generate [generates] the marker by using the generated control word and CP information and [encrypts] encrypt the resulting marker by means of [the encoded] an encoding key. Finally, a multiplexing and transmitting step 7 multiplexes the scrambled audio and video bit strips and encrypted marker to transmit the result.

The audio and video signal receiving and recording process is performed in such a manner that the marker is detected from the transmitted bit strips and is decrypted by means of the [encoded] encoding key and analyzed. Thus, it is determined whether the copy is permitted or not, the detected marker is updated accordingly [to update the detected marker to be recorded on a video tape], and the control word is

produced from the marker to carry out the descrambling and display the signals on a monitor. As a result, [in which] the audio and video signals transmitted from the program producer are recorded or displayed in accordance with the marker.

[More specifically, as shown in] FIG. 2[,] shows the audio and video signal receiving and recording process in detail. As shown, the process includes [is performed by] marker detecting steps 11 and 12 for detecting the marker by demultiplexing the transmitted bit strips, and decrypting the marker by means of the [encoded] encoding key, and a marker analyzing step 13 for analyzing the detected marker to determine whether [the] a copy is permitted or not and for detecting the control word. Then, the transmitted audio and video bit strips are descrambled and decoded [by] using the detected control word to supply the audio and video signals in audio and video decoding steps 14 and 15. Thereafter, the detected marker is updated and encrypted by means of the [encoded] encoding key [to be inserted in case of permitting the copy after analyzing the marker in a] and reinserted in the transmitted audio and video bit strips in marker inserting steps 16, 17 and 18 if copying is permitted.

The above-stated process will be described in detail below.

To begin with, the program producer encodes the audio and video bit strips 1, generates the control word for scrambling 2, and scrambles the encoded audio and video bit strips by means of the generated control word 6.

Also, the CP information for preventing the illegal copy is generated 3, [and] the marker is generated by using the generated control word and CP information 4, and the coded key is utilized to perform the encryption 5.

Finally, the scrambled audio and video bit strips and encrypted marker are multiplexed 7 to be transmitted for the program recording or reproduction.

The transmitted bit strips are demultiplexed to detect the marker 11. The encoding [, and the encoded] key is utilized to perform the decryption and the decrypted marker is output 12. The detected and decrypted marker is analyzed to determine whether the copy is permitted or not and the control word is detected 13.

The detected control word is used for descrambling and decoding the transmitted audio and video bit strips to provide the audio and video signals to the monitor [to be displayed] for display 14 and 15.

In addition, when it is determined that [the] a copy is permitted after analyzing the marker, the detected marker is updated, [to be encrypted] re-encrypted by means of the [encoded] encoding key, and the result is inserted to the audio and video bit strips to be recorded 16, 17 and 18.

Here, a position of inserting the marker will be observed with reference to FIG. 3.

The transmitted bit strips [consists] consist of transport packets of a fixed length, i.e., 188 bytes, in which a transport header is displaced on the preceding stage of the bit strips. The transport header is divided into a field of a fixed length of 4 bytes and an adaptation field of a variable length. Then, a transport-private-data field exists as one field within the adaption field. The transport-private-data field consists of an ID field and the encrypted marker. The ID field functions as [a] an identifier for informing that the transport-private-data field is a field utilized for the copy prevention method according to the present invention, and the encrypted marker following the ID field embodies the copy prevention function of the present invention.

When the marker is decrypted by means of the [encoded] encoding key, the decrypted marker is divided into a CP

information area including [recorded with] the CP information for preventing the illegal copy, a control word area including [recorded with] the control word CW for descrambling, and a reserved area.

That is, the decrypted marker is formed of 8 bytes consisting of the CP information area of one byte, the reserved area of three bytes and control word area of four bytes.

At this time, the CP information is formatted by including a generational copy control field which restricts the number of permitted copies [permitting the copy] of the program. The generational copy control field [, which] is formed of an allowable generational field for limiting the copy number of the program and a current generational field representing a current generation of the duplicated program.

Next, the marker analyzing step 13 of the audio and video receiving and recording process will be described in detail.

The marker analyzing step 13 is carried out by the CP information detecting step of detecting the CP information for preventing the illegal copy from the detected marker, a copy number limiting step of comparing the allowable generation of the allowable generational field for restricting the number of permitting the copy of the program and the current generation of the current generational field representing the current generation of the duplicated program within the detected CP information to determine whether the copy is permitted or not, and the control word detecting step of detecting the control word from the detected marker for executing the descrambling.

In other words, the CP information for preventing [the] an illegal copy is detected from the detected marker, and the allowable generation of the allowable generational field for limiting the copy number of the program is compared with the current generation of the current generational field representing the current generation of the duplicated program within the detected CP information to determine whether the copy is permitted or not, so that the program is recorded in case of permitting the copy. Otherwise, [otherwise the] reproduction cannot be executed in case of inhibiting the copy, even though the recording is attained.

Next, the control word for descrambling is detected from the detected marker.

Here, the step of limiting the copy number is carried out by comparing the allowable generation of the allowable generational field with the current generation of the current generational field to determine whether the allowable generation is the current generation, inhibiting the copy when it is determined that the allowable generation is below the current generation, and permitting the copy when it is determined that the allowable generation is not below the current generation [to proceed to the marker insertion step].

The copy number limiting step will be described below.

When the allowable generation is below the current generation after comparing the allowable generation of the allowable generational field preset by the program producer with the current generation of the current generational field representing the current copy number, the copy number exceeds the copy number preset by the program producer. Thus, copying cannot be [the copy cannot be further] permitted.

At this time, in order to inhibit the copy, the control word is destructed or is not output, which blocks [to block the] reproduction of [after performing] the copy. This is because the audio and video bit strips are recorded under the state of being scrambled, the scrambled audio and video bit strips cannot be descrambled without the control word.

Therefore, by destructing the control word, the reproduction and display cannot be achieved even though the

audio and video bit strips are recorded; [to] thereby [have] having the same effect [of] as impeding the recording of them.

At this time, since the control word is periodically changed of an [in the] interval of 0.6 second, the reproduction is impeded by destructing the succeeding control word even after accomplishing the recording.

Also, a control track within the video tape may be destructed to inhibit the copy when the recording medium is a video tape.

On the other hand, the marker is positioned on the private data field within the bit strips whenever the control word is changed.

Here, since the control word is periodically changed, the marker including the control word is received whenever the control word is changed [to be supplied].

Meantime, the marker inserting step is performed by updating the marker when the copy is permitted after analyzing the marker 16, encrypting the updated marker by means of the encoded key 17, and replacing the encrypted marker with the [following] marker to be inserted 18.

In other words, if the copy is permitted after analyzing the marker, the current generation of the current generational field is augmented by one to update the marker 16. That is, the CP information including the updated current generational field obtained by augmenting the current generation by one is summed with the control word to be the updated marker.

The updated marker is encrypted by means of the encoding key and is inserted to replace [encoded key to be replaced with] the succeeding marker [and inserted] 17. More specifically, as the marker is supplied whenever the control word is changed, it is inserted whenever the control word is changed.

In other [word] words, as shown in FIG. 3, the detection of the encrypted marker and the replacement of the updated marker should be accomplished altogether on time basis.

Meanwhile, the [encoded] encoding key for encrypting and decrypting the marker is transmitted via a separate transmission line in a predetermined time interval and is stored to be utilized, thereby perfectly preventing the illegal copy.

That is, the marker encrypted by the [encoded] encoding key is transmitted and recorded together with the bit strips. Here, the control word for descrambling the scrambled audio and video bit strips is included in the marker, so that the marker should be primarily decrypted to obtain the control word. However, since the [encoded] encoding key for decrypting the marker is periodically changed, it is impossible to decrypt the marker without the [encoded] encoding key. Accordingly, it is further difficult to illegally obtain the control word.

As shown in FIG. 4, the copy prevention apparatus of the digital magnetic recording/reproducing system according to the present invention includes a marker detecting/inserting section 21, a descrambler 24, a marker analyzing/processing section 22 and a buffer section 23.

Marker detecting/inserting section 21 detects the marker from the received bit strips, and inserts [to output] the updated marker, i.e., the updated and encrypted marker, from buffer section 23 to the bit strips.

Marker analyzing/processing section 22 utilizes the [encoded key] encoding keys to decrypt and analyze the encrypted marker from marker detecting/inserting section 21, thereby providing the control word CW for descrambling the bit strips. Then, the decrypted marker is updated and encrypted by the [encoded] encoding key [to be] for output.

Buffer section 23 buffers control word CW and the updated and encrypted marker IEM from marker

analyzing/processing section 22, so that the updated and encrypted marker IEM is supplied to be inserted in marker detecting/inserting section 21.

Descrambler 24 descrambles the bit strips output via marker detecting/inserting section 21 by means of the control word CW from buffer section 23 to supply the result to the monitor to be displayed or to, for example, a DVCR to record the bit strips [inserted] with the marker.

Here, the [encoded] encoding key is transmitted via the separate transmission line [in] at a predetermined time interval and is stored as the copy prevention method of the digital magnetic recording/reproducing system according to the present invention to double a copyright protection effect.

Referring to FIG. 3, the structure of the transport bit strips and marker will be described prior to describing the operation of the copy prevention apparatus of the digital magnetic recording/reproducing system constructed as above.

In the copy prevention apparatus of the digital magnetic recording/reproducing system, the marker is placed on the transport-private-data field within the bit strips, and the CP information area recorded with the CP information for preventing the illegal copy and the control word area recorded with the control word CW for descrambling are included thereto as shown in FIG. 3, like the copy prevention method.

Here, the CP information is formatted by including the generational copy control field for restricting the number of permitted copies of the program, which is formed of the allowable generational field for limiting the copy number of the program and the current generational field representing the current generation of the duplicated program.

The marker is formed of 8 bytes consisting of the CP information area of one byte and control word area of four bytes.

Hereinbelow, an operation of the copy prevention apparatus of the digital [magnetic] recording/reproducing system according to the present invention will be briefly described with reference to FIG. 4.

First, a process of displaying the input bit strips on the monitor will be described.

The input bit strips are supplied to marker analyzing/processing section 22 under the state that the marker is detected and encrypted in marker detecting/inserting section 21.

Encrypted marker EM is decrypted by means of the [encoded] encoding key to be analyzed in marker analyzing/processing section 22. At this time, the control word is detected from the analyzed marker [to be buffered] via buffer section 23 for descrambling the bit strips and is supplied to descrambler 24.

The bit strips, after [detecting] the detection of the marker in marker detecting/inserting section 21, are descrambled in descrambler 24 in accordance with the control word from buffer section 23, and provided to the monitor [to be displayed] for display.

Next, a process of recording the input bit strips via, for example, the DVCR will be described.

The process of detecting and analyzing the marker from the input bit strips is executed in the same manner.

That is, the input bit strips [is] are supplied to marker analyzing/processing section 22 under the state that the marker is detected and [encrypted] decrypted in marker detecting/inserting section 21.

Encrypted marker EM is decrypted by means of the [encoded] encoding key in marker analyzing/processing section 22 to detect the control word. At this time, the recording can be performed or not in accordance with the

result of the analysis. If the recording is not permitted, the detected control word is destructed to impede the reproduction even though the recording can be attained. Otherwise, the current generation of the current generational field within the marker is augmented by one to update the marker, [so that] the [encoded] encoding key is utilized to encrypt the marker, and [to supply] the result is supplied to buffer section 23.

The updated and encrypted marker is buffered in buffer section 23 and is supplied to marker detecting/inserting section 21 to be inserted to the input bit strips.

Meantime, the control word is periodically changed in the interval of 0.6 second, and the marker is placed on the transport-private-data field within the bit strips whenever the control word is changed.

Consequently, the updated and encrypted marker [is replaced with] replaces the succeeding marker [to be inserted].

The bit strips [inserted] with the updated and encrypted marker pass through descrambler 24 intact and are output to be recorded in the DVCR.

The detailed construction and operation of the copy prevention apparatus in the digital magnetic recording/reproducing system formed as above will be described with reference to the accompanying drawings.

FIG. 5 is a detailed construction view showing the copy prevention apparatus of FIG. 4, which will be described below.

Marker detecting/inserting section 21 includes a marker detector 31 which detects the encrypted marker from the input bit strips and supplies the detected marker to marker analyzing/processing section 22 and a marker detection flag signal for informing of the position of the encrypted marker within the bit strips to descrambler 24. The flag is [to be] used as a reference signal [of] for initializing descrambler 24 while outputting the bit strips. In addition to marker detector 31, a marker inserter 32 inserts the updated and encrypted marker from buffer section 23 into [to] the bit strips from marker detector 31 in accordance with the marker detection flag signal from marker detector 31. The [to output the] result is output to descrambler 24.

Marker analyzing/processing section 22 has a marker decoder 34 for decrypting the encrypted marker from marker detector 31 of marker detecting/inserting section 21 by means of the [encoded] encoding key, and a marker analyzer 34 [for analyzing] analyzes the CP information within the marker from marker decoder 34 to output the control word to buffer section 23 when the copy is permitted while outputting a control signal for updating the marker. Additionally, a marker updating/encoding unit 35 updates the marker from marker decoder 34 in accordance with the control signal from marker analyzer 34 to encrypt the marker by means of the [encoded] encoding key to output the result to buffer section 23.

Here, marker analyzing/processing section 22 further includes an encoding key storage unit (not shown) for storing the [encoded] encoding key and to output the [result] encoding key to marker decoder 33 and marker updating/encoding unit 35.

Also [Besides], marker analyzer 34 compares the allowable generation of the allowable generational field for restricting the number of permitting the copy of the program with the current generation of the current generational field representing the current generation of the duplicated program to determine whether [the] a copy is permitted or not.

Buffer section 23 includes a marker buffer 36 for temporally storing the updated and encrypted marker from marker analyzing/processing section 22 to supply it to marker detecting/inserting section 21, and a control word buffer 37 for temporally storing the control word from marker

analyzing/processing section 22 to supply it to descrambler 24.

An operation of the copy prevention apparatus of the digital magnetic recording system according to the present invention constructed as above will be described with reference to [FIG. 6] FIGS. 6A-6G.

FIG. 6A is a timing chart of the transmitted bit strips, FIG. 6B [is of] illustrates the marker detection flag m-det-flag, FIG. 6C [is of] illustrates the control word CW(i) from marker analyzer 34, FIG. 6D illustrates [is of] the updated and encrypted marker IEM(i) from marker updating/encoding unit 35, FIG. 6F [is of] illustrates the updated and encrypted marker IEM(i) from marker buffer 36, and FIG. 6G [is of] illustrates the control word CW(i) from control word buffer 37.

Encrypted marker EM(i) is included in the transmitted bit strips.

The transmitted bit strips including encrypted marker EM(i) [is] are formed as shown in FIG. 6A, which is supplied to marker detector 31 to detect encrypted marker EM(i) to be supplied to marker decoder 33. Also, marker detector 31 generates marker detection flag signal m-det-flag for informing of the position of [the encrypted marker at] the encrypted marker EM(i) [portion] as shown in FIG. 6B, so that the generated signal is supplied to marker inserter 32 together with the bit strips including encrypted marker EM(i). Also, marker detection flag m-det-flag is supplied to descrambler 24 to be utilized as the reference signal for initializing descrambler 24 by control word CW(i-1) from control word buffer 37.

Encrypted marker EM(i) is decrypted by the encoding key in marker decoder 33 [to be] and is supplied as decrypted marker M(i).

Decrypted marker M(i) is analyzed in marker analyzer 34 to determine whether the copy is permitted or not. In other words, marker analyzer 34 compares the CP information within decrypted marker M(i), i.e., the allowable generational field with the current generational field, and determines to permit the copy when the allowable generational field is not below the current generational field.

When the copy is permitted [as above], marker analyzer 34 slightly delays control word CW(i), which is a part of decrypted marker M(i), to be supplied to control word buffer 37, as shown in FIG. 6C. At this time, marker analyzer 34 [provide] provides the control signal to marker updating/encoding unit 35 to control the updating of the marker.

That is, marker decoder 33 [form] forms decrypted marker M(i) from encrypted marker EM(i) after a delay [delaying a] time required for the decode, and the marker analyzer 34 generates control word CW(i) from decrypted marker M(i) [in marker analyzer 34].

At this time, control word CW(i) is transmitted to control word buffer 37 to be stored until it is utilized in descrambler 24.

Decrypted marker M(i) from marker decoder 33 is updated in accordance with the control signal from marker analyzer 34 in marker updating/encoding unit 35.

That is, the updated data is the data recorded on the current generational field within the marker, which is obtained by adding one to the previously recorded current generation.

The marker updated as described above is encrypted, i.e., encoded, in accordance with the [encoded] encoding key to be supplied to marker buffer 36 as shown in FIG. 6D, slightly delayed with respect to control word CW(i) from marker analyzer 34 as shown in FIG. 6C. In more detail, the encrypted marker M(i) from marker decoder 33 is supplied to marker

updating/encoding unit 35 to be generated as marker IEM(i), which is updated and encrypted after a delay [delaying the] time required for the encoding, and marker IEM(i) is [to be] supplied to marker buffer 36.

Here, the point of generating updated and encrypted marker IEM(i) and control word CW(i) from marker updating/encoding unit 35 and marker analyzer 34 does not coincide with a point of utilizing updated and encrypted marker IEM(i) and control word CW(i) in marker inserter 32 and descrambler 24, i.e., the points of performing the replaceable insertion and initialization of descrambler 24 do not coincide with each other. Thus, updated and encrypted marker IEM(i) and control word CW(i) from marker updating/encoding unit 35 and marker analyzer 34 are temporally stored in marker buffer 36 and control word buffer 37 for that time.

As shown in FIG. 6E, updated and encrypted marker IEM(i) temporally stored in marker buffer 36 and synchronized to be output is inserted by marker inserter 32 into [to] the bit strips from marker detector 31.

In more detail, marker inserter 32 receives the bit strips having encrypted marker EM(i) and marker detection flag signal m-det-flag from marker detector 31, and receives updated and encrypted marker IEM(i) which will be replaceably inserted into [to] the position of encrypted marker EM(i) from marker buffer 36, so that updated and encrypted marker IEM(i) is replacably inserted to the position of marker detection flag signal m-det-flag in the transmitted bit strips including encrypted marker-EM(i) as shown in FIG. 6E.

In other words, marker inserter 32 inserts updated and encrypted marker IEM(i) from marker buffer 37 replacing encrypted marker EM(i+1) at the position of producing marker detection flag signal m-det-flag.

Here, the replacably inserted marker IEM(i) is formed from the immediately detected preceding encrypted marker. Accordingly, as shown in FIG. 6E, the marker IEM(i) is stored in marker buffer 37 for a certain period [to be] and then provided to marker inserter 32.

As shown in FIG. 6F, control word CW(i-1) is temporally stored in control word buffer 37 to be synchronized prior to being output and is utilized for descrambling the transmitted bit strips from marker inserter 32 in descrambler 24.

At this time, descrambler 24 uses marker detection flag signal m-det-flag from marker detector 31 as the reference signal for initializing based on control word CW(i-1) from control word buffer 37.

More specifically, descrambler 24 must be initialized by control word CW(i-N) from control word buffer 37 during a period from the point of generating encrypted marker EM(i), i.e., from a position of detecting marker detecting flag signal m-det-flag to the point before starting payload of a transport packet, where N is a natural number greater than zero. Here, control word CW(i-N) is a control word formed from encrypted marker EM(i-N) transmitted before encrypted marker EM(i) as many as N times. The natural number `N` allows for arbitrarily controlling the initializing point of descrambler 24.

In the copy prevention method and apparatus of the digital [magnetic] recording/reproducing system according to the present invention as described above, a program supplier can select the copy prevention function, and the field defined within a GA format is utilized. As the result, a separate format transformation apparatus for the copy prevention function is not required, and there is no increase in data amount to be recorded to perform the copy prevention function without converting, for example, the general digital VCR.

While the present invention has been particularly shown and described with reference to particular embodiment thereof, it will be understood by those skilled in the art that various changes in form and details may be effected therein without departing from the spirit and scope of the invention as defined by the appended claims.

What is claimed is:

[1. A copy prevention method of a digital magnetic recording/reproducing system comprising:

an audio and video signal transmitting process of encrypting a marker formed by a control word for scrambling audio and video bit strips and copy prevention information for preventing an illegal copy by means of an encoding key, and multiplexing said marker with said audio and video bit strips scrambled by said control word, and

an audio and video signal receiving/recording process of detecting said marker from said transmitted bit strips, decrypting and analyzing the detected marker by means of an encoded key to determine whether copy is permitted or not, updating said detected marker to be recorded on a video tape, and generating said control word from said marker to perform a descrambling and supply the audio and video signals to be displayed on a monitor]

[2. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 1, wherein said marker is placed on a transport-private-data field within said bit strips.]

[3. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 2, wherein said marker is comprised of a copy prevention information area recorded with said copy prevention information for preventing said illegal copy, and a control word area recorded with said control word for descrambling.]

[4. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 3, wherein said marker is formed of 8 bytes.]

[5. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 4, wherein said copy prevention area is formed of one byte.]

[6. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 4, wherein said control word area is formed of four bytes.]

[7. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 3, wherein said copy prevention information is formatted by including a generational copy control field for restricting the number of permitting said copy of a program.]

[8. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 7, wherein said generational copy control field comprises:

an allowable generational field for restricting the copy number of said program; and

a current generational field representing a current generation of a duplicated program.]

[9. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 1, wherein said audio and video transmitting process comprises:

an audio and video bit-strip encoding step of encoding said audio and video bit strips;

a control word generating step of generating said control word for scrambling.

a scrambling step for scrambling said encoded audio and video bit strips by means of said generated control word;

a copy prevention information generating step of generating said copy prevention information for preventing said illegal copy;

a marker generating and encrypting step of generating said marker by means of said generated control word and copy prevention information and encrypting said marker by means of said encoded key; and

a multiplexing and transmitting step of multiplexing to transmit said scrambled audio and video bit strips and encrypted marker.]

[10. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 1, wherein said audio and video signal receiving/recording process comprises:

a marker detecting step of demultiplexing said transmitted bit strips to detect said marker, and decrypting said marker by means of said encoded key;

a marker analyzing step of analyzing said detected marker to determine whether said copy is permitted or not, and detecting said control word;

an audio and video decoding step of descrambling and decoding said transmitted audio and video bit strips by means of said detected control word, and outputting said audio and video signals; and

a marker inserting step of updating said detected marker and encrypting said updated marker by means of said encoded key to insert the result when it is determined that said copy is permitted after analyzing said marker.]

[11. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 10, wherein said marker analyzing step comprises:

a copy prevention information detecting step of detecting said copy prevention information for preventing said illegal copy from said detected marker;

a copy number restricting step of comparing an allowable generation of said allowable generational field and a current generation of said current generational field representing said current generation for restricting the number of permitting said copy of said program within said detected copy prevention information, and determining whether said copy is permitted or not to process the result; and

a control word detecting step of detecting said control word for descrambling from said detected marker.]

[12. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 11, wherein said copy number restricting step comprises:

comparing said allowable generation of said allowable generational field with said current generation of said current generational field to determine whether said allowable generation is below said current generation;

inhibiting said copy when it is determined that said allowable generation is below said current generation; and

permitting said copy when it is determined that said allowable generation is not below said current generation, and proceeding to said marker inserting step.]

[13. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 12, wherein said step of inhibiting said copy is performed by destructing said control word or impeding an output of said control word to block a reproduction after recording.]

[14. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 10, wherein said control word is periodically changed.]

[15. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 14, wherein said control word is changed in the interval of 0.6 second.]

[16. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 14, wherein said marker is placed on said transport-private-data field within said bit strips whenever said control word is changed.]

[17. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 16, wherein said marker inserting step comprises the steps of:

updating said marker when the analysis of said marker determines to permit said copy;

encrypting said updated marker by means of said encoded key; and

replacably inserting said encrypted marker with a succeeding marker.]

[18. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 1, wherein said encoded key is transported via a separate transmission line to be stored.]

[19. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 18, wherein said encoded key is transported via said separate transmission line for a prescribed time interval.]

[20. A copy prevention apparatus of a digital magnetic recording/reproducing system comprising:

an encrypted marker detecting and inserting part for detecting a marker from input bit strips, and inserting an updated marker to said bit strips to output the result;

a marker analyzing and processing part for decrypting and analyzing the encrypted marker from said marker detecting and inserting part by means of an encoded key, outputting a control word for descrambling said bit strips, and updating and encrypting the decrypted marker by means of said encoded key to output the result;

a buffer part for buffering said control word and updated and encrypted marker from said marker analyzing and processing part, and inserting said updated and encrypted marker in said marker detecting and inserting part; and

a descrambler for descrambling said bit strips provided via said marker detecting and inserting part by means of said control word from said buffer part.]

[21. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said encoded key is transported via a separate transmission line to be stored.]

[22. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 21, wherein said encoded key is transported via said separate transmission line for a prescribed time interval.]

[23. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said marker is placed on a transport-private-data field within said bit strips whenever said control word is changed.]

[24. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 23, wherein said marker is comprised of a copy prevention information area recorded with said copy prevention information for preventing said illegal copy, and a control word area recorded with said control word for descrambling.]

[25. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24, wherein said marker is formed of 8 bytes.]

[26. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 25, wherein said copy prevention area is formed of one byte.]

[27. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 25, wherein said control word area is formed of four bytes.]

[28. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24, wherein said copy prevention information is formated by including a generational copy control field for restricting the copy number of a program.]

[29. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 28, wherein said generational copy control field comprises:

an allowable generational field for restricting the number of permitting the copy of a program; and

a current generational field representing a current generation of a duplicated program.]

[30. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said control word is periodically changed.]

[31. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 30, wherein said control word is changed in the interval of 0.6 second.]

[32. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 30, wherein said marker is placed on a transport-private-data field within said bit strips whenever said control word is changed.]

[33. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 30, wherein said marker detecting and inserting part replacably inserts said updated marker with a succeeding marker.]

[34. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24, wherein said marker detecting and inserting part comprises:

a marker detecting section for detecting to output said encrypted marker from said input bit strips to said marker analyzing and processing part, outputting a marker detection flag signal for informing of the position of said encrypted marker within said bit strips to said descrambler to be used as a reference signal of initializing said descrambler, and outputting said bit strips; and

a marker inserting section for inserting said updated and encrypted marker from said buffer part to said bit strips from said marker detecting section in accordance with said marker detection flag signal from said marker detecting section to output the result to said descrambler.]

[35. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24, wherein said marker analyzing and processing part comprises:

a marker decoding section for decrypting said encrypted marker from said marker detecting and inserting part by means of said encoded key;

a marker analyzing section for analyzing said copy prevention information within said marker from said marker decoding section, and outputting said control word to said buffer part and a control signal for updating said marker when said copy is permitted; and

a marker updating and encoding section for updating said marker from said marker decoding section in accordance with said control signal from said marker analyzing section, and encrypting said updated marker by means of said encoded key to output the result to said buffer part.]

[36. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 35, wherein said marker analyzing and processing part further comprises an encoded key storage section for storing said encoded key to output it to said marker analyzing section and marker updating and encoding section.]

[37. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 35,

wherein said marker analyzing section compares an allowable generation of an allowable generational field with a current generation of a current generational field representing a current generation of a duplicated program to determine whether said copy is permitted or not.]

[38. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said buffer part comprises:

a marker buffer for temporally storing said updated and encrypted marker from said marker analyzing and processing part and outputting the result to said marker detecting and inserting part; and

a control word buffer for temporally storing said control word from said marker analyzing and processing part and outputting the result to said descrambler.]

39. A method for transmitting digital data, comprising:

scrambling digital data; and

transmitting the scrambled digital data, identification information, and copy prevention information as part of a data group, the data group including a header and the header including the identification information, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

40. The method of claim 39, wherein the scrambling step scrambles the digital data based on control data such that the control data controls a parameter of the scrambling operation.

41. The method of claim 40, wherein the transmitting step transmits the control data as part of the data group.

42. The method of claim 41, further comprising:

encrypting the control data prior to the transmitting step; and wherein

the transmitting step transmits the encrypted control data as part of the data group.

43. The method of claim 42, wherein the encrypting step encrypts the control data based on a key.

44. The method of claim 39, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

45. A method for transmitting digital data, comprising:

scrambling digital data; and

recording the scrambled digital data, identification information, and copy prevention information as part of a data group, the data group including a header and the header including the identification information, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

46. The method of claim 45, wherein the scrambling step scrambles the digital data based on control data such that the control data controls a parameter of the scrambling operation.

47. The method of claim 46, wherein the transmitting step transmits the control data as part of the data group.

48. The method of claim 47, further comprising:

encrypting the control data prior to the transmitting step; and wherein

the transmitting step transmits the encrypted control data as part of the data group.

49. The method of claim 48, wherein the encrypting step encrypts the control data based on a key.

50. The method of claim 45, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital

data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

51. A method of processing protected digital data, comprising:

receiving a data group including identification information, control data and scrambled digital data, the data group also having a header and the header including the identification information, the identification information indicating that at least a portion of the data group has a data structure for copy prevention; and

descrambling the scrambled digital data based on the control data.

52. The method of claim 51, wherein

the receiving step receives copy prevention information as part of the data group, and further including,

performing a copy prevention function based on the copy prevention information.

53. The method of claim 51, wherein

the receiving step receives encrypted control data as part of the data group; and further including,

decrypting the encrypted control data prior to the descrambling step.

54. The method of claim 53, wherein the decrypting step decrypts the control data using a key.

55. The method of claim 51, wherein the copy prevention information includes one of current generation information and allowable generation information, the current

generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

56. A copy protected recording medium having a data structure for controlling a copy prevention operation of a reproducing device, comprising:

a data group area including an identification area, a copy prevention area and a digital data area;

the identification area including identification information indicating that at least a portion of the data group has a data structure for copy prevention;

the copy prevention area including copy prevention information for controlling a copy prevention operation of a reproducing device; and

the digital data area including scrambled digital data.

57. The recording medium of claim 56, wherein the data group area further includes a control data area, the control data area storing control data for descrambling the scrambled digital data.

58. The recording medium of claim 57, wherein the control data area stores encrypted control data.

59. The recording medium of claim 56, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

60. A method for protecting digital data, comprising:

encrypting control data, the control data having been used to control a parameter of a scrambling operation for scrambling digital data; and

transmitting the scrambled digital data and a marker, the marker including the control data and copy prevention information.

61. The method of claim 60, wherein the transmitting step transmits the scrambled digital data and the marker as a data group.

62. The method of claim 61, wherein the transmitting step transmits identification information as part of the data group, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

63. The method of claim 60, wherein the copy prevention information indicates a number of permitted copies of the digital data.

64. The method of claim 60, wherein the encrypting step encrypts the control data using a key.

65. A method for protecting digital data, comprising:

encrypting control data, the control data having been used to control a parameter of a scrambling operation for scrambling digital data; and

transmitting the scrambled digital data and the control data as part of a data group, the data group including a header and the header including the control data.

66. The method of claim 65, wherein the transmitting step transmits copy prevention information as part of the data group.

67. The method of claim 66, wherein the copy prevention information indicates a number of permitted copies of the digital data.

68. The method of claim 65, wherein the encrypting step encrypts the control data using a key.

69. The method of claim 65, wherein the transmitting step transmits identification information as part of the data group, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

[11] Patent Number: 5,689,559
[45] Date of Patent: Nov. 18, 1997

Assistant Examiner—Carmen D. White
Attorney, Agent, or Firm—John P. White

[57] ABSTRACT

A copy prevention method and apparatus of a digital magnetic recording/reproducing system performs the copy prevention function by encoding to insert a marker involving copy prevention function information and executing the function and allows a program supplier to realize a desired copy prevention function of various patterns, in which the marker formed by a control word for scrambling audio and video bit straps and copy prevention information for preventing an illegal copy is encrypted by an encoded key to be multiplexed with the audio and video bit strips scrambled by the control word. The marker transmitted is detected from the bit strips to be decrypted and analyzed by the encoded key to determine whether the copy is permitted or not, so that the detected marker is updated to be recorded on a video tape and the control word is produced from the marker to perform the descrambling to supply the result to a monitor to be displayed. Thus, the program supplier selects the copy prevention function, and a separate format converting apparatus is not required since a field defined within a GA format is utilized while an existing DVCR is not need to be changed for performing the copy prevention function as the data amount to be recorded is not increased.

38 Claims, 5 Drawing Sheets

FIG. 1

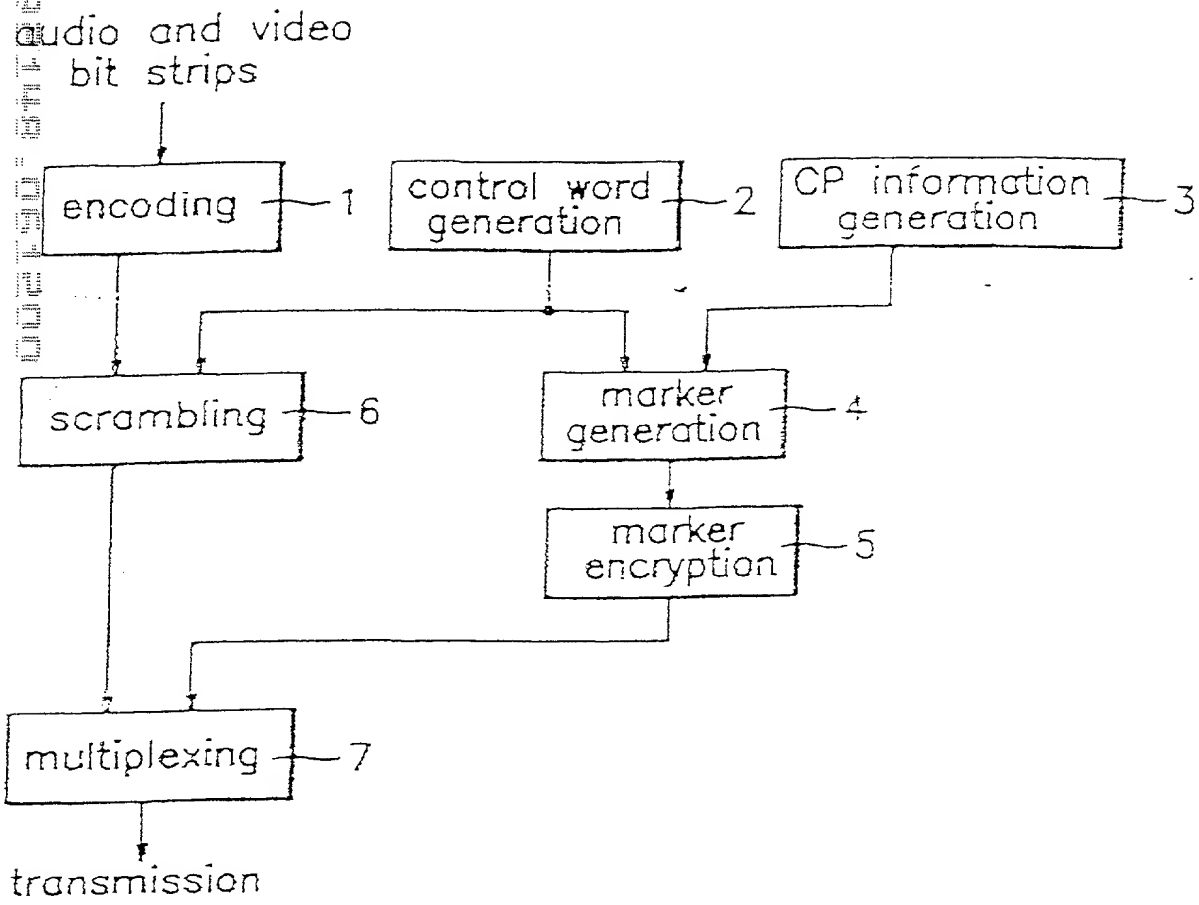

audio and video bit strips
encoding
1
control word generation
2
CP information generation
3
scrambling
6
marker generation
4
marker encryption
5
multiplexing
7
transmission

FIG.2

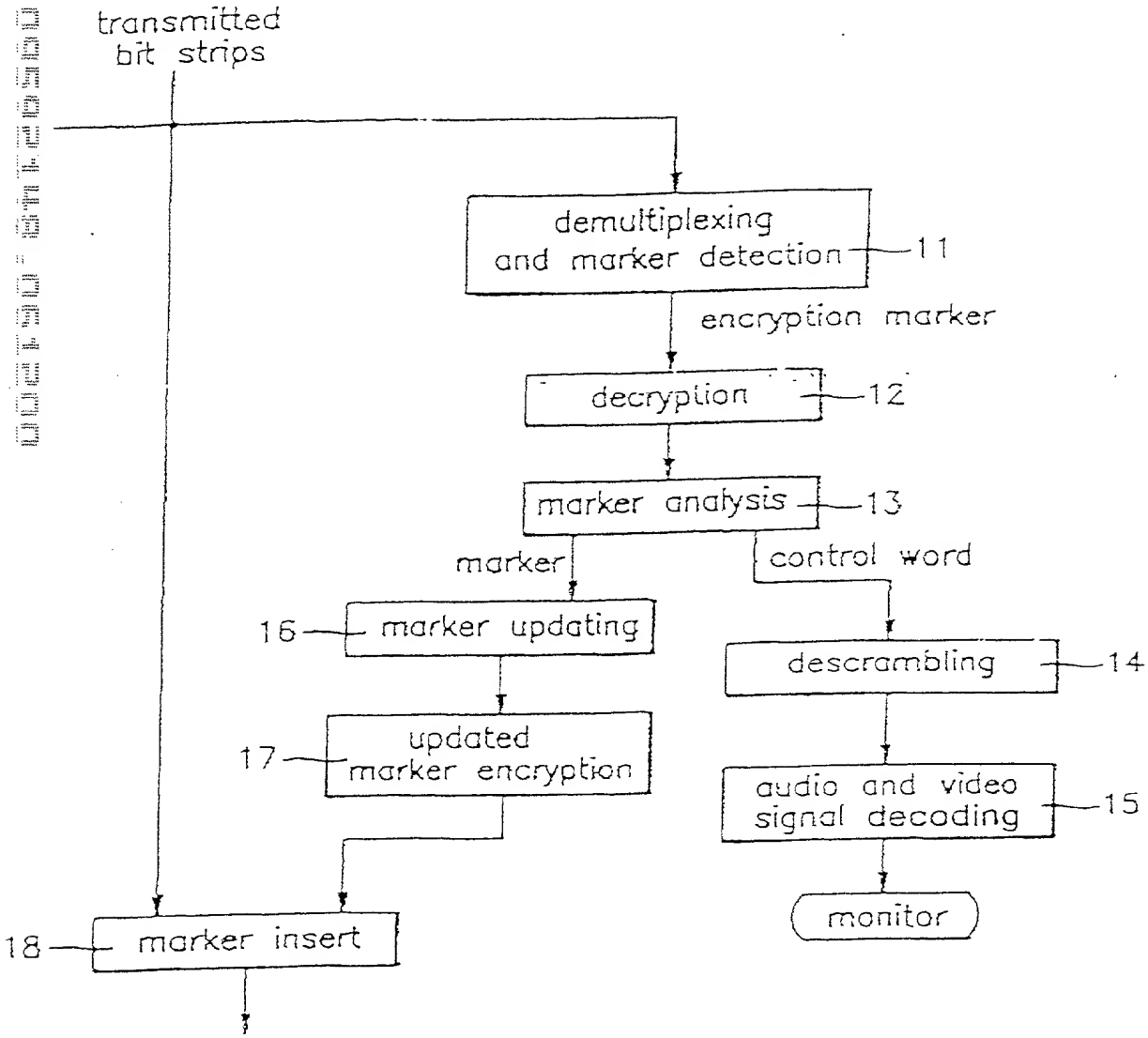

transmitted bit strips
demultiplexing and marker detection
11
encryption marker
decryption
12
marker analysis
13
marker
control word
16
marker updating
descrambling
14
17
updated marker encryption
audio and video signal decoding
15
monitor
18
marker insert

FIG.3

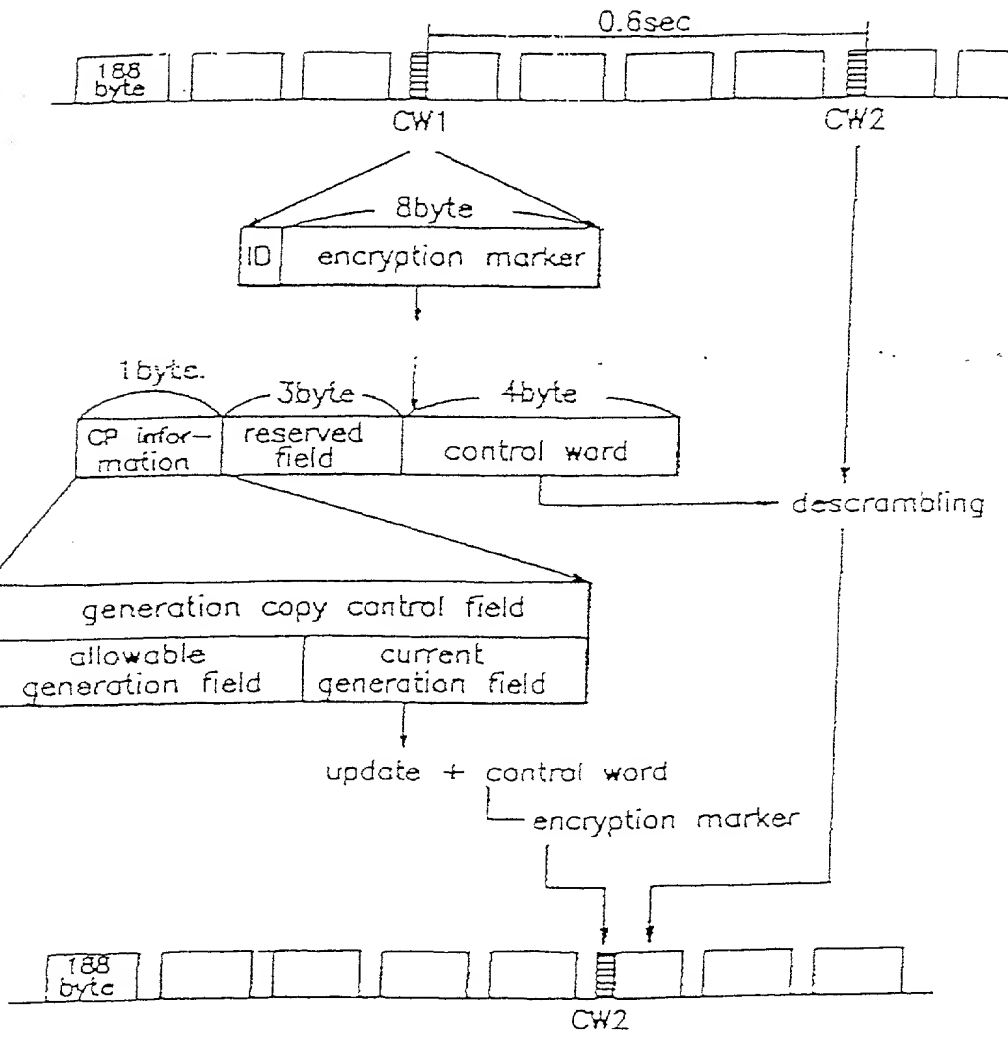

0.6sec
188 byte
CW1
CW2
8byte
ID
encryption marker
1byte.
3byte
4byte
CP information
reserved field
control word
descrambling
generation copy control field
allowable generation field
current generation field
update + control word
encryption marker
188 byte
CW2

FIG.4

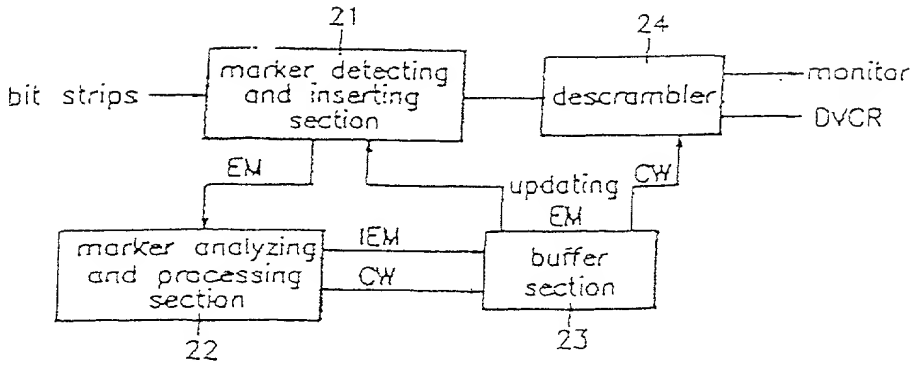
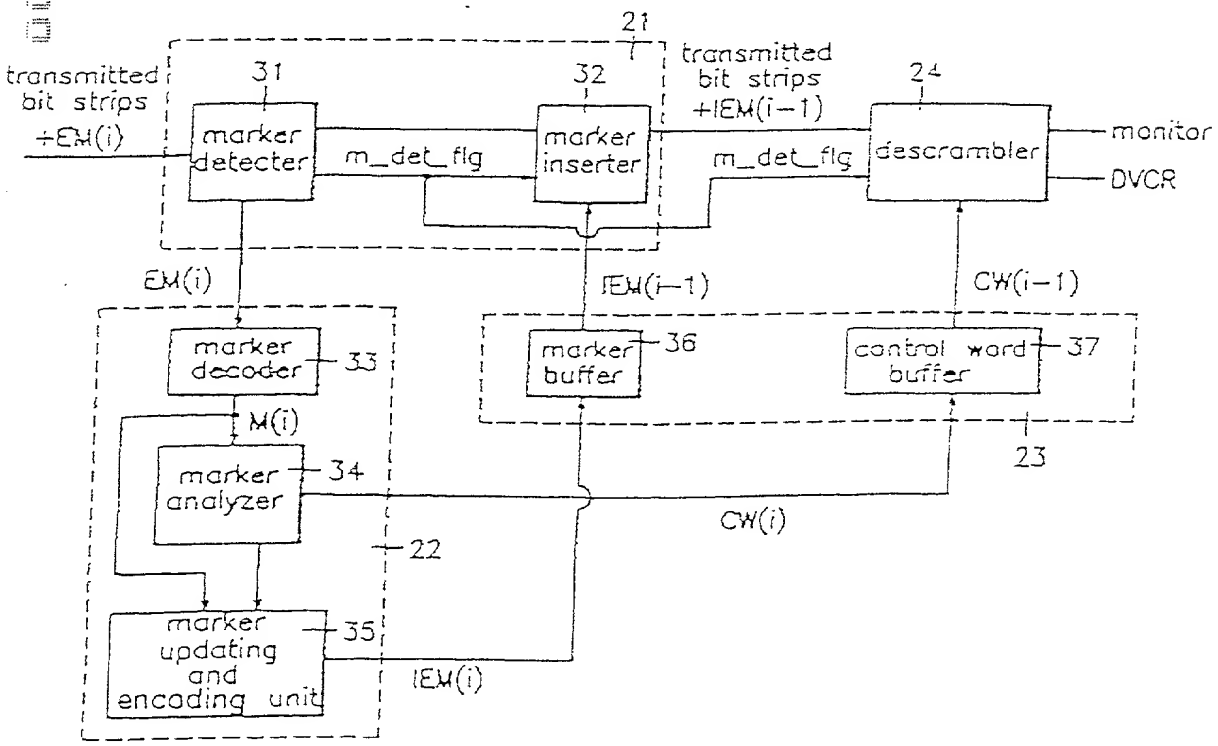

21
24
bit strips
marker detecting and inserting section
descrambler
monitor
DVCR
EM
updating CW
EM
IEM
CW
marker analyzing and processing section
buffer section
22
23

FIG.5


21
transmitted bit strips +EM(i)
31
32
transmitted bit strips +IEM(i-1)
24
marker detecter
m_det_flg
marker inserter
m_det_flg
descrambler
monitor
DVCR
EM(i)
IEM(i-1)
CW(i-1)
marker decoder
33
M(i)
marker analyzer
34
22
marker updating and encoding unit
35
IEM(i)
marker buffer
36
control word buffer
37
23
CW(i)

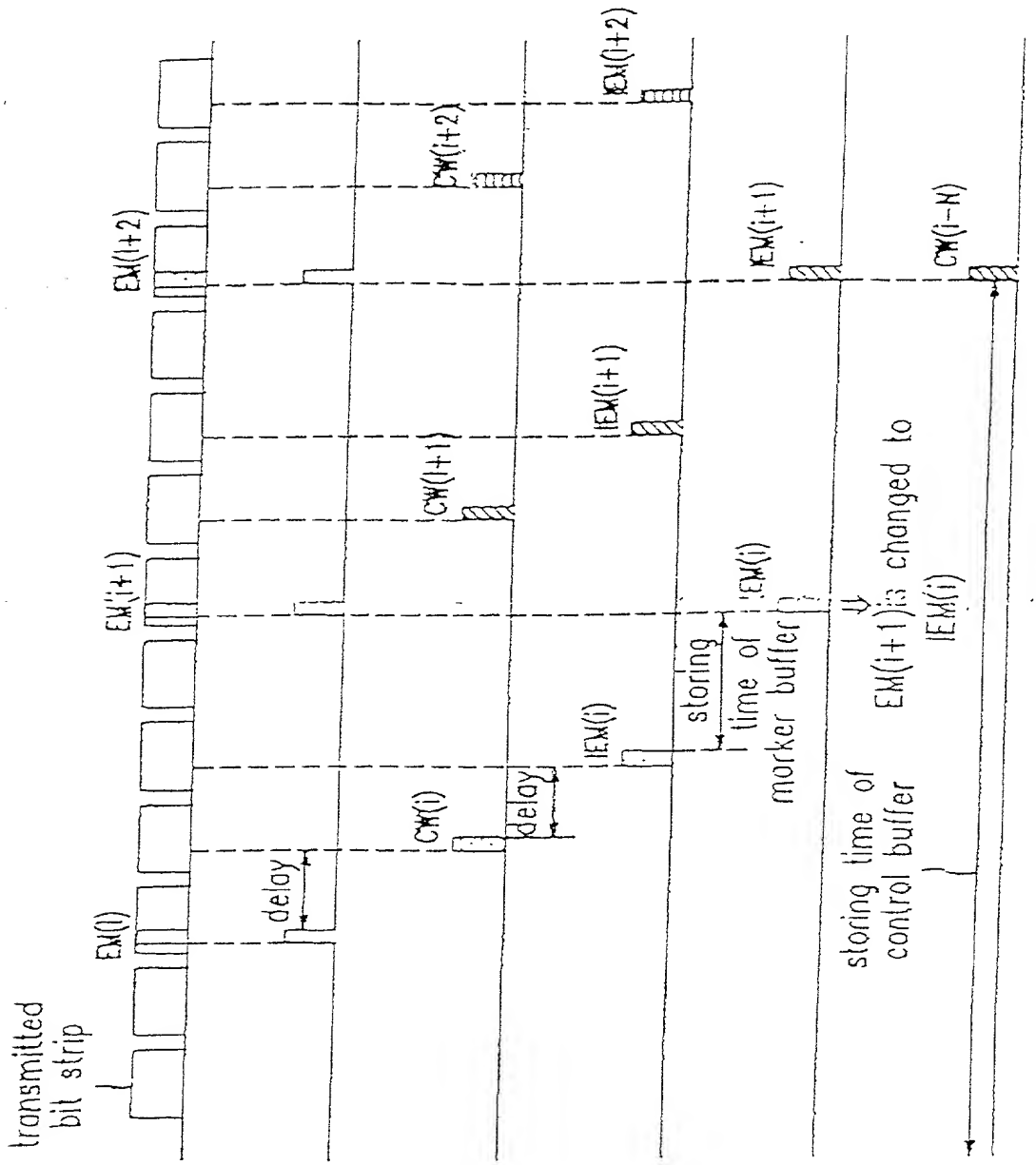


FIG.6A

FIG.6B

FIG.6C

FIG.6D

FIG.6E

FIG.6F

PATENT
2950-0160P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS: Tae Joon PARK

APPLICATION. NO.: NEW CONTINUATION APPLICATION OF USSN 09/094,575, WHICH IS A REISSUE APPLICATION OF U.S. Pat. No. 5,689,559

FILING DATE: (Issued: November 18, 1997)

FOR: COPY PREVENTION METHOD AND APPARATUS OF A DIGITAL MAGNETIC RECORDING/REPRODUCING SYSTEM

COMBINED REISSUE DECLARATION AND POWER OF ATTORNEY

As the below named inventor, I hereby declare as follows:

That my name, residence, post office address and citizenship is as indicated below.

That I have reviewed and understand the contents of the attached reissue application including original claims 1-38 and the newly submitted claims 39-70.

That I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

That I verily believe that I am the original, first and only inventor of the invention described and claimed in United States Patent No. 5,689,559 entitled "COPY PREVENTION METHOD AND APPARATUS OF A DIGITAL MAGNETIC RECORDING/REPRODUCING SYSTEM" and in the foregoing specification for which invention I respectfully solicit a reissue patent.

That I do not know and do not believe that the same invention was ever known or used before my invention or discovery thereof; or patented or described in any printed publication in any country before my invention or discovery thereof, or more than one (1) year prior to the filing of my original application for United States Letters Patent No. 5,689,559 of which that is an application for reissue; or in public use or on sale in the United States of America for more than one (1) year prior to the filing of the original application; or that the invention has been patented or made the subject of an inventor's certificate issued before the date of the original application in any country foreign to the United States of America on an application filed by me or my legal representatives or assignees more than twelve (12) months prior to said original application and that no application for patent or inventor's certificate have been filed by me or my legal representatives or assignees in any country foreign to the United States of America before the application of the original patent.

That I verily believe that there are errors in the original patent which make such original patent partially inoperative by reason of claiming less than I had a right to claim and that such errors occurred without any deceptive intent.

That the claims of original application were directed to a copy prevention method of a digital magnetic recording/reproducing system or a copy prevention apparatus of a digital magnetic recording/reproducing system.

That while I originally recognized the importance of the aspects of the invention, I did not understand the importance of claiming and thus, when the original application was prepared, I failed to recognize that not all of the details required for realizing all of the aspects were needed and thus, I failed to recognize that

the more basic concepts of the invention disclosed in the specification were not covered by the original claims.

That this lack of adequately claiming the invention was due in part to the numerous features that were part of the disclosed embodiment of my invention, without considering how to broadly recite a particular aspect of my invention.

That I did not advise the U.S. attorneys, and accordingly, they did not fully recognize, that varying levels of importance of each of the aspects of the invention. That I, while recognizing the relative significance of each of the aspects of the invention, did not understand the importance of claiming and thus, I did not realize that I had claimed less than I was entitled to.

That when I executed the Declaration of the original application, I reviewed the application carefully for accuracy, but did not recognize the importance of broadly presenting other less significant aspects of the invention and the claims or that individual aspects could be claimed alone. That it was not until after the original Letters Patent issued that I discovered that the original presented claims did not adequately define my invention.

That for this reason, there was an error in the original patent claims which rendered the original patent partially inoperative by failure to adequately claim these aspects of my invention.

That with respect to claim 1, which recites a copy prevention method of a digital magnetic recording/reproducing system, one error is the recitation of both an audio and video signal transmitting process and an audio and video signal receiving/recording process. That new independent method claims 39, 45, 61 and 66

are directed to one of transmitting and recording to resolve this error. And, that new independent claim 51 is directed to a method of processing digital data to further resolve this error.

That claims 40-44, 46-50, 52-56, 62-65, and 67-70, dependent on claims 39, 45, 51, 61, and 66, respectively, are necessary to further define the basic elements of the invention recited in independent claims 39, 45, 51, 61, and 66.

That further errors related to all original claims in U.S. Patent 5,689,559 are the failure to provide patent protection for the recording medium of the original patent. That independent claim 57 resolves this error.

That claims 58-60, dependent on claim 57, are necessary to further define the basic elements of the invention recited in independent claim 57.

That the above cited errors are not comprehensive of all the errors, but merely reflect some of the errors.

That, however, all errors being corrected in the reissue application up to the time of filing this Declaration arose without deceptive intent on the part of the Applicant.

That this is a Continuation Application of Reissue Application 09/094,575 filed June 12, 1998 and priority is hereby claimed on Reissue Application 09/094,575.

In summary, claims 1-38 are inadequate to protect my invention as these claims do not encompass the more basic concepts of my invention recited in new independent claims 39, 45, 51, 57, 61 and 66. This inadequacy of claims 1-38 requires the addition of claims 39-70.

Upon review of the prior art cited during the examination of the original application, I do not believe that any of documents disclose or suggest the invention as set forth in any of the claims 39-70, and that I am entitled to the more comprehensive protection offered by the added claims 39-70. As such, I believe that all of claims 39-70 are necessary to protect my invention with claims of varying scope, and to correct for the insufficiencies of claims 1-38.

Applicant hereby appoints the following as his attorneys, with full power of substitute and revocation, to prosecute this application and transact all business in the United States Patent and Trademark Office in connection therewith, and request that all correspondence with respect to this application be directed to:

BIRCH, STEWART, KOLASCH & BIRCH, LLP
P.O. Box 747
Falls Church, Virginia 22040-0747 USA

Terrell C. Birch	(Reg. No. 19,382)	Raymond C. Stewart	(Reg. No. 21,066)
Joseph A. Kolasch	(Reg. No. 22,463)	James M. Slattery	(Reg. No. 28,380)
Bernard L. Sweeney	(Reg. No. 24,448)	Michael K. Mutter	(Reg. No. 29,680)
Charles Gorenstein	(Reg. No. 29,271)	Gerald M. Murphy, Jr.	(Reg. No. 28,977)
Leonard R. Svensson	(Reg. No. 30,330)	Terry L. Clark	(Reg. No. 32,644)
Andrew D. Meikle	(Reg. No. 32,868)	Marc S. Weiner	(Reg. No. 32,181)
Joe McKinney Muncy	(Reg. No. 32,334)	Donald J. Daley	(Reg. No. 34,313)
Robert J. Kenney	(Reg. No. N/A)	John A. Castellano	(Reg. No. 35,094)
Gary D. Yacura	(Reg. No. 35,416)		

WHEREFORE, the Petitioner hereby offers to surrender, upon the allowance of said application, the original of said Letters Patent and prays that Letters Patent be reissued to Petitioner for the invention of patent claims 1-38 with the newly presented claims 39-114.

The undersigned declares further that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to true; and further that these statements are made with the knowledge that

willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize validity of the application or any reissue patent issuing thereon.

Tae Joon Park Signature: TAE JOON PARK

Date: JUN. 9, 2000

Residence: Seoul, Republic of Korea
Citizenship: Korean
Post Office Address: 20-88 Soongin-1-Dong, Jongro-Gu, Seoul 110-551, KOREA